Access control system and method for smart cards

Patent Number:	DE3736190
Publication date:	1988-05-05
Inventor(s):	SHIRAISHI TAKAYOSHI (JP); SASAKI RYOICHI (JP); TAKARAGI KAZUO (JP); KURASHIKI NOBUHIRO (JP); TANIGUCHI NOBUHIRO (JP)
Applicant(s):	HITACHI LTD (JP)
Requested Patent:	DE3736190
Application Number:	DE19873736190 19871026
Priority Number (s):	JP19860251641 19861024
IPC Classification:	G06F12/14; G06K19/06
EC Classification:	G06F1/00N1D1, G06F21/00N1D1, G07F7/10D2M
Equivalents:	JP63106888

Abstract

The invention concerns a system and method for controlling access to smart cards, to each of which several users have access. After the smart card has been delivered by a manufacturer, a system administration centre accesses it and enters an access procedure, access area and access authorisation for each further user into the smart card. The further users can have access to the smart card only by matching the access procedure, access area and access authorisation which have been set by the system administration centre. The smart card (100(a)) has a data input/output device (101 (a)), a data processing device (102(a)) and a data storage device (103(a)). The access procedure, access area and access authorisation are set by the system administration centre, in collaboration with the data processing device (102(a)) on the smart card (100(a)). A control device which is provided as part of the data processing device (102(a)) of the smart card monitors the correctness of the access procedure, access area and access authorisation on the user side, and takes suitable security measures on unauthorised access. For example, these may consist of inverting an invalidity recording code or of blocking operation.

(19) BUNDESREPUBLIK DEUTSCHLAND

(12) **Offenlegungsschrift**

(11) **DE 37 36 190 A1**

(51) Int. Cl. 4:
G 06 F 12/14
G 06 K 19/06

DEUTSCHES PATENTAMT

(21) Aktenzeichen: P 37 36 190.2
(22) Anmeldetag: 26. 10. 87
(43) Offenlegungstag: 5. 5. 88

(30) Unionspriorität: (32) (33) (31)
24.10.86 JP P 251641/86

(71) Anmelder:
Hitachi, Ltd., Tokio/Tokyo, JP

(74) Vertreter:
Beetz sen., R., Dipl.-Ing.; Beetz jun., R., Dipl.-Ing. Dr.-Ing.; Timpe, W., Dr.-Ing.; Siegfried, J., Dipl.-Ing.; Schmitt-Fumian, W., Privatdozent, Dipl.-Chem. Dr.rer.nat., Pat.-Anwälte, 8000 München

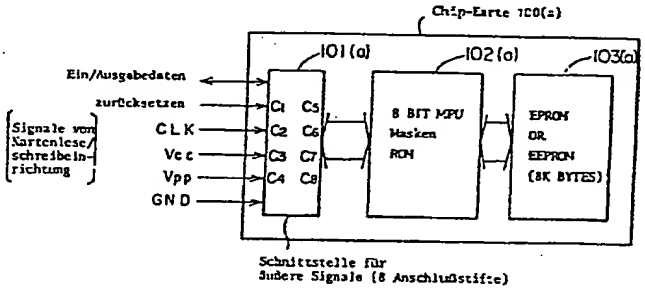
(72) Erfinder:
Takaragi, Kazuo; Kurashiki, Nobuhiro, Yokohama, JP; Sasaki, Ryoichi, Fujisawa, JP; Shiraishi, Takayoshi, Chigasaki, JP; Taniguchi, Nobuhiro, Hadano, JP

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Zugriffssteuersystem und -Verfahren für Chip-Karten

Die Erfindung betrifft ein System und Verfahren zur Steuerung des Zugriffs zu Chip-Karten, zu denen jeweils mehrere Benutzer Zugriff haben. Nach Lieferung der Chip-Karte von einer Herstellerfirma greift eine Systemverwaltungszentrale zur Chip-Karte zu und setzt eine Zugriffsprozedur, einen Zugriffsbereich und eine Zugriffsberechtigung für die jeweiligen weiteren Benutzer in die Chip-Karte. Die weiteren Benutzer können zur Chip-Karte nur in Übereinstimmung mit der durch die Systemverwaltungszentrale gesetzten Zugriffsprozedur, dem Zugriffsbereich und der Zugriffsberechtigung zugreifen. Die Chip-Karte (100(a)) weist eine Datenein/Ausgabeeinrichtung (101(a)), eine Datenverarbeitungseinrichtung (102(a)) und eine Datenspeichereinrichtung (103(a)) auf, wobei das Setzen der Zugriffsberechtigung, des Zugriffsbereichs und der Zugriffsprozedur seitens der Systemverwaltungszentrale in Zusammenarbeit mit der Datenverarbeitungseinrichtung (102(a)) auf der Chip-Karte (100(a)) erfolgt.
Eine als Teil der Datenverarbeitungseinrichtung (102(a)) der Chip-Karte vorgesehene Steuereinrichtung überwacht die Richtigkeit der gesetzten Zugriffsprozedur, des Zugriffsbereichs und der Zugriffsberechtigung seitens der Benutzer und ergreift geeignete Sicherheitsmaßnahmen bei unberechtigtem Zugriff, die z. B. im Invertieren eines Ungültigkeitserfassungskennzeichens oder im Blockieren des Betriebs bestehen können.

FIG. 1a



DE 3736190 A1

Patentansprüche

1. Verfahren zur Zugriffssteuerung zu einer Chip-Karte, die eine Ein/Ausgabe-Einrichtung (101*(a)*), eine Datenverarbeitungseinrichtung (102*(a)*) und eine Datenspeichereinrichtung (103*(a)*) aufweist und zu der mehrere Benutzer zugreifen können, **gekennzeichnet durch** die aufeinanderfolgenden Schritte:

a) Setzen einer Zugriffsberechtigung, einer Zugriffsprozedur und eines Zugriffsbereichs auf der Chip-Karte durch eine Systemverwaltungszentrale; und
b) Freigabe des Zugriffs durch einen Benutzer, der danach zur Chip-Karte zugreifen will nur wenn der Benutzer die durch die Systemverwaltungszentrale gesetzte Zugriffsprozedur und/oder den Zugriffsbereich und/oder die Zugriffsberechtigung innerhalb des gesamten durch die Systemverwaltungszentrale gekennzeichneten Zugriffsbereichs einhält.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Zugriffsprozedur und der Zugriffsbereich nur durch die Systemverwaltungszentrale gesetzt werden können.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß sobald ein Benutzer versucht die zuvor durch die Systemverwaltungszentrale gesetzte Zugriffsprozedur und/oder Zugriffsbereich zu ändern, als Gegenmaßnahmen eine Betriebsunterbrechung, ein Datenlöschen oder die Inversion eines Ungültigkeitserfassungskennzeichens durchgeführt werden.

4. System zur Steuerung des Zugriffs zu einer Chip-Karte (100*(a)*), die eine Datenein/Ausgabeeinrichtung (101*(a)*), eine Datenverarbeitungseinrichtung (102*(a)*) und eine Datenspeichereinrichtung (103*(a)*) aufweist, wobei mehrere Benutzer zur Chip-Karte zugreifen können, gekennzeichnet durch

— eine Initialisierungseinrichtung (202, 203, 205, 206), die in Zusammenwirken mit der Datenverarbeitungseinrichtung (102*(a)*) und der Datenspeichereinrichtung (103*(a)*) der Chip-Karte (100*(a)*) die Zugriffsprozedur, den Zugriffsbereich und die Zugriffsberechtigung zur Chip-Karte getrennt von dem Zugriffsbereich, der Zugriffsprozedur und der Zugriffsberechtigung durch die jeweiligen Benutzer setzt, wobei die Initialisierungseinrichtung Teil einer Systemverwaltungszentrale (201) ist, und
— eine als Teil der Datenverarbeitungseinrichtung (102*(a)*) realisierte Steuereinrichtung, die die durch die Initialisierungseinrichtung getrennt spezifizierten Zugriffsberechtigungen, -Bereiche und -Prozeduren seitens der Benutzer überwacht, ungültige Zugriffe erfaßt und bei unberechtigtem Zugriff seitens der jeweiligen Benutzer Sicherheitsmaßnahmen steuert.

Beschreibung

Die Erfindung betrifft ein Zugriffssteuersystem und -Verfahren für ein Chip-Karten-System, bei dem mehrere Benutzer zu auf einer Chip-Karte gespeicherter Information zugreifen. Eine Chip-Karte besteht aus einem in seinen Abmessungen mit einer Kreditkarte identischen Plastikplättchen, das eine oder mehrere hochintegrierte Schaltungs-Chips aufweist.

Bei bekannten Chip-Karten-Systemen wird die Chip-Karte nur von dem einen Besitzer verwendet, wie beim Kreditkartensystem. Um die Möglichkeit einer Chip-Karte besser auszunützen, kann eine solche vorteilhafterweise von mehreren Benutzern wie in einem Personal-Computer-System verwendet werden.

Bei einem solchen Chip-Karten-System, bei dem mehrere Benutzer einer Chip-Karte zugeordnet sind, speichert ein auf der Chip-Karte enthaltener Speicher sowohl individuelle Information für den einzelnen Benutzer, als auch Information, die von allen Benutzern gemeinsam verwendet wird. Deshalb kann jeder zum Zugriff autorisierte Benutzer die gemeinsame Information leicht auslesen oder ändern. Außerdem könnte im Falle mehrerer Benutzer die zum Zugriff berechtigenden Regeln nicht genau beachten, selbst wenn die Zugriffsberechtigung mittels einer Kennummer oder dergleichen überprüft wird, die Kennummer einer dritten Person bekannt werden, die somit eine Zerstörung oder den Verlust von den Benutzern zugeteilter Information ermöglichen könnte.

Es ist deshalb Aufgabe der Erfindung, ein Zugriffssteuersystem und -Verfahren für Chip-Karten für einen Fall anzugeben, bei dem die Chip-Karte von mehreren Benutzern verwendet wird, wobei die Sicherheit insbesondere gegen unbeabsichtigtes oder fälschliches Löschen von auf der Chip-Karte gespeicherter Information verbessert werden soll.

Zur Lösung der obigen Aufgabe wird, um die Sicherheit bei der Benutzung der Chip-Karte zu garantieren, erfindungsgemäß eine Steuerung der Zugriffsberechtigung und des Zugriffsbereichs jeweils für die Systemverwaltung und den gewöhnlichen Benutzer vorgesehen. Dabei wird unter Systemverwaltung die Spezifikation der Registrierung, des Löschens, der Zugriffsprozedur und des Zugriffsbereichs für den gewöhnlichen Benutzer verstanden.

Letzterer ist eine zur Benutzung der Chip-Karte in Übereinstimmung mit den von der Systemverwaltung auferlegten Beschränkungen autorisierte Personen.

Außerdem hat jeder Benutzer seinen eigenen Bereich, und deshalb ist für den anderen Benutzer die Berechtigung zum Zugriff zu diesem Bereich ebenfalls beschränkt.

Erfindungsgemäß wird eine neue von der Farik gelieferte Chip-Karte einer zur Registrierung des der Systemverwaltung zugeordneten Bereichs einer Operation durch die Systemverwaltung unterworfen.

Damit kann eine gewöhnliche Benutzerperson zu dem für die Systemverwaltung vorgesehenen Bereich nicht mehr zugreifen.

Dann wird die Registrierung der Benutzer durch die Systemverwaltung durchgeführt. Bei dieser Operation wird ein Bereich, zu dem ein jeweiliger Benutzer Zugriff hat, sowie Prozeduren und Beschränkungen für den jeweiligen Benutzer spezifiziert.

Diese Spezifikationen werden durch eine Informationsschreiboperation; z. B. zum Einschreiben einer Kennummer für den jeweiligen Benutzer in einen Bereich, zu dem nur die Systemverwaltung Zugriff hat, ausgeführt. Nach dieser Initialisierungsoperation haben die Benutzer die Berechtigung zur Chip-Karte zuzugreifen.

Bei jedem Zugriff zur Chip-Karte muß der jeweilige

Benutzer die durch die Systemverwaltung vorgeschriebene Zugriffsprozedur einhalten, beispielsweise eine dem Benutzer eigene Kennummer eingeben. Außerdem kann ein jeweiliger Benutzer auch nach Beendigung der vorgeschriebenen Zugriffsprozdur, sobald zur Chip-Karte zugegriffen werden kann, zu keinem andern als dem von der Systemverwaltung zugewiesenen Bereich zugreifen. Das heißt, daß auch der Benutzer versucht Daten zu überschreiben, beispielsweise die dem Benutzer auferlegten Beschränkungen entfernen, weil eine solche ungültige Operation durch die Chip-Karte erfaßt wird, die eine entsprechende Gegenmaßnahme ergreift, beispielsweise die Operation verriegelt. Genauso kann die Chip-Karte, wenn ein Benutzer unberechtigt Information aus einem nur der Systemverwaltung zugeteilten Bereich auslesen will, Gegenmaßnahmen, die beispielsweise eine Verarbeitung zum Löschen von Information ergreifen.

Mit dem beschriebenen erfindungsgemäßen Zugriffssteuersystem läßt sich ein unberechtigtes Auslesen, eine Änderung der Information vermeiden und außerdem kann mittels des erfindungsgemäßen Zugriffssteuersystems für die Informationsübertragung die Geheimhaltung und Beachtung der Privatsphäre bei der Verwendung der Chip-Karte durch mehrere Benutzer erreicht werden.

Im folgenden wird die Erfindung anhand der Zeichnung in Ausführungsbeispielen näher beschrieben. Es zeigt

Fig. 1a ein Blockschaltbild einer erfindungsgemäßen Ausführungsart der Chip-Karte;

Fig. 1b schematisch ein Speicherbelegungsplan eines ROM- Speichers eines EEP ROM-Speichers auf der Chip-Karte;

Fig. 2 ein Blockschaltbild eines Ausführungsbeispiels eines Schlüsselübertragungssytems; und

Fig. 3 ein Flußdiagramm eines Protokolls der Schlüsselübertragung.

Fig. 1a zeigt zunächst schematisch ein Blockschaltbild des Aufbaus der Chip-Karte gemäß einem Ausführungsbeispiel der Erfindung. Eine Chip-Karte **100***(a)* enthält zwei hochintegrierte Schaltkreise.

Die Eingabe/Ausgabe-Daten werden über einen I/O-Abschnitt **101***(a)* so übertragen, daß sie von bzw. zu einem EPROM (oder EEPROM) **103***(a)* über einen Mikroprozessor **102***(a)* transferiert werden. Die 8-Bit-Mikroprozessoreinheit (weiterhin MPU) **102***(a)* enthält ein 4-Kilobyte Masken-ROM als Programmspeicherbereich. Das im Masken-ROM gespeicherte Programm wird zur Abwicklung des Datenverkehrs mit einer äußeren Einrichtung und zur Zugriffssteuerung in dem Datenspeicher (weiterhin EPROM) **103***(a)* verwendet.

Das EPROM **103***(a)* ist ein nichtflüchtiger Speicher, der die Benutzerdaten speichert und eine Kapazität von acht Kilobyte haben kann. Dieser Speicher besteht aus einem EPROM-Speicherbaustein, bei dem die Daten elektrisch programmierbar und durch Ultraviolettlicht löschbar sind.

Ein alternativ verwendbares EEPROM ist ein elektrisch löschbarer und programmierbarer und nicht flüchtiger Speicher, der ebenfalls die Speicherkapazität acht Kilobyte haben kann.

Nun wird ein Ausführungsbeispiel der Erfindung beschrieben, das bei einer Nachrichtenverkehrsoperation angewendet wird.

Fig. 1b zeigt schematisch einen Speicherbelegungsplan der gemäß der Erfindung konfigurierten Chip-Karte. In diesem Falle ist der Speicherbereich des EPROMs auf der Chip-Karte in einen Bereich, zu dem nur die Systemverwaltung Zugriff hat und der ein Speicherbereich **101** für eine Systemverwaltungskennummer, einen Speicherbereich **102** für eine gewöhnliche Benutzerkennummer sowie einen Speicherbereich **103** für eine Terminalkennummer umfaßt, und einen Speicherbereich, zu dem sowohl die Systemverwaltung als auch ein gewöhnlicher Benutzer Zugriff hat und der die Nachrichtenspeicherbereiche *(A)* und *(B)* **104** und **105** umfaßt. Die Zugriffsberechtigung des gewöhnlichen Benutzers wird von der Systemverwaltung geeignet bestimmt. Diese Zugriffsberechtigung ist auf eine Leseoperation aus dem Bereich *(A)* **104** und auf eine Schreib- und Leseoperation für den Bereich *(B)* **105** beschränkt.

Außerdem sind die Bereiche **101** bis **105** bei Verwendung eines EEPROMs oder dergleichen überschreibbar, und die darin gespeicherten Inhalte werden von einem im ROM-Speicherbereich **106** gespeicherten Chip-Karten-Zugriffssteuerprogramm gesteuert. Das Steuerprogramm wird durch einen Befehl von einem Terminal gestartet und danach werden Operationen, wie z. B. eine Wiedergewinnungs- und Entscheidungsoperation durch das Steuerprogramm ausgeführt und dadurch die im Speicherbereich **107** des EEPROMs gespeicherten Inhalte kontrolliert.

Das heißt, daß der am Terminal eingegebene Befehl über den I/O-Abschnitt **101***(a)* der Chip-Karte **100***(a)* gemäß **Fig.** 1a zur MPU **102***(a)* übertragen und darin dekodiert wird, die das durchführende Programm beginnend mit einer vorgegebenen Adresse, nämlich seiner ersten Adresse, ablaufen läßt. Das Programm weist Nachrichtenverkehrssteuerfunktionen **1061**, eine Zugriffsberechtigungsentscheidungsfunktion **1063**, eine Unterscheidungsfunktion für ein benutztes Terminal und eine EEPROM-Auslese- und Einschreibfunktion **1064**, auf (**Fig.** 1b).

Anhand der **Fig.** 2, die ein Ausführungsbeispiel darstellt, wie ein die mit dem erfindungsgemäßen Zugriffssteuersystem und Zugriffssteuerverfahren arbeitende Chip-Karte einsetzendes Nachrichten- bzw. Informationsaustauschsystem konfiguriert ist und der **Fig.** 3, die ein Flußdiagramm darstellt, das eine Verarbeitungsprozedur beschreibt, die in dem in **Fig.** 2 gezeigten erfindungsgemäß konfigurierten System ein Schlüsselliefersystem bewirkt, wird die Erfindung weiterhin näher beschrieben.

Anhand des in **Fig.** 3 dargestellten Flußdiagramms werden die Operationen der in den **Fig.** 1a, 1b und 2 dargestellten Teile erläutert.

Schritt **301**:
Sobald ein Nachrichtenaustausch angefordert wird, überträgt ein Benutzer **207** seine Kennummer **212** und die Kennummer **211** eines Terminals **205**, an dem eine Kartenlese/Schreibeinrichtung **206** angeschlossen ist zu einer Zentrale **201**.

Schritt **302**:
Die Zentrale **201** empfängt die Nachrichtenaustauschanforderung vom Benutzer **207** und startet die Vorbereitung einer Chip-Karte **204** für den Nachrichtenaustausch.

Schritt **303**:
Die Zentrale **201** schreibt eine Kennummer **208** der Zentrale **201** in den auf der Chip-Karte vorgesehenen Speicherbereich **101** für die Systemverwaltungskennnummer in diesem Anfangszustand. Dadurch wird die Zentrale **201** für diese Chip-Karte zur Systemverwaltung.

Schritt 304:
Um die Terminals einzuschränken, die Zugriff zur Chip-Karte 204 haben, schreibt die Zentrale 201 eine Kennnummer 210 eines benutzten Terminals 202 und eine Kennummer 211 des vom Benutzer 207 betriebenen Terminals 205 in den Speicherbereich 103 der Chip-Karte 204, der für die Terminalkennummer vorgesehen ist.

Schritt 305:
Die Zentrale 201 schreibt die Kennummer 212 des Benutzers in den Speicherbereich 102 der Chip-Karte, der für eine gewöhnliche Benutzerkennummer vorgesehen ist.

Schritt 306:
Die Zentrale 201 schreibt eine Nachricht in den Speicher, bereich *(A)* 104 der Chip-Karte 204 und liefert dann die Chip-Karte an den Benutzer 207 mittels eines Liefernetzwerks für materielle Güter (beispielsweise durch eine Einschreib-Postsendung).

Schritt 307:
Der Benutzer 207 empfängt die Chip-Karte 204 und gibt diese in die Kartenlese/Schreibeinrichtung 206, die mit dem Terminal 205 verbunden ist, ein.

Schritt 308:
Der Benutzer 207 schreibt seine eigene Kennummer 212 in die Chip-Karte 204 ein.

Schritt 309:
Ein Chip-Karten-Zugriffssteuerprogramm, das in dem ROM-Bereich 106 auf der Chip-Karte 204 gespeichert ist, sucht den Speicherbereich 102 für die gewöhnliche Benutzerkennummer ab um zu prüfen, ob die Kennummer 212 des Benutzers 207 bereits eingeschrieben ist.

Schritt 310:
Falls die Kennummer 212 bereits eingeschrieben ist, fordert das Steuerprogramm das Terminal 205 auf, die Terminalkennummer 211 zu senden.

Schritt 311:
Das Steuerprogramm sucht den Speicherbereich 103 für die Terminalkennummer um zu prüfen, ob die Terminalkennummer 211 des Terminals 205, mit dem der Benutzer 207 arbeitet, bereits eingeschrieben wurde.

Schritt 312:
Falls die Kennummer 211 bereits eingschrieben wurde, liest der Benutzer 207 die in den Nachrichtenspeicherbereich *(A)* 104 auf der Chip-Karte 204 eingeschriebene Nachricht 209.

Schritt 313:
Der Benutzer schreibt eine Benutzernachricht 213 in den Speicherbereich *(B)* 105 der Chip-Karte 204 und schickt dann die Chip-Karte 204 an die Zentrale 201 durch das Liefernetzwerk 214 für materielle Güter.

Schritt 314:
Die Zentrale 201 empfängt die Chip-Karte 204 und gibt die Karte 204 in die Kartenlese/Schreibeinrichtung 203, die mit dem Terminal 202 verbunden ist.

Schritt 315:
Die Zentrale 201 gibt der Chip-Karte 204 ihre eigene Kennnummer ein.

Schritt 316:
Das Steuerprogramm prüft, ob die Kennummer 201 der Zentrale bereits in den Speicherbereich 101 für die Systemverwaltungskennummer eingeschrieben ist.

Schritt 317:
Falls die Kennummer 208 bereits eingeschrieben wurde, fordert das Steuerprogramm vom Terminal 201 die Übertragung der Terminalkennummer 210 an.

Schritt 318:
Das Steuerprogramm sucht in dem Speicherbereich 103 die Terminalkennummer um zu prüfen, ob die Terminalkennummer 210 der Zentrale 201 bereits registriert wurde.

Schritt 319:
Falls die Terminalkennummer 210 bereits registriert ist, liest die Zentrale 201 die Nachricht 213 aus dem Nachrichtenspeicherbereich *(B)* 105 auf der Chip-Karte 204.

Darauffolgend springt das Steuerprogramm zum Schritt 320, falls die Prüfung in den Schritten 309, 311, 316 und 319 einen unregistrierten Fall ergibt, um die Verarbeitung zu unterbrechen, und dann wird Schritt 321 ausgeführt, damit der Benutzer 207 von der Situation benachrichtigt wird.

Durch die Erfindung lassen sich folgende vorteilhafte Wirkungen erzielen:

1. Schutz gegen unberechtigtes Auslesen und Änderung der Daten beim Liefern der Chip-Karte.

Wenn die Chip-Karte mittels des Liefernetzwerks für materielle Güter, beispielsweise durch die Post, verschickt wird, kann die Chip-Karte möglicherweise in die Hände einer dritten Person gelangen, die mit böswilliger Absicht in den Versandweg eingreift.

In diesem Falle kann die dritte Person zur Chip-Karte nicht zugreifen, da die Chip-Karte selbst Kennummer, Terminalkennummer und dergleichen prüft, wie dies anhand der Schritte 309, 311, 316 und 318 beschrieben wurde, und weil die dritte Person den Prüfvorgang nicht weiß. Folglich kann auf diese Weise das unberechtigte Auslesen und Ändern der Daten auf dem Versandweg verhindert werden.

2. Schutz vor Änderung einer Nachricht der Zentrale durch den Benutzer.

Der gewöhnliche Benutzer oder eine dritte Person, die dessen Kennummer, die Terminalkennummer und dergleichen, die auf der Chip-Karte gespeichert sind, weiß, kann folglich zur Chip-Karte zugreifen. Da jedoch die Information oder Nachricht der Zentrale in einen Bereich eingeschrieben wird, zu dem nur die Systemverwaltung Zugriff hat, kann diese Nachricht oder Information von einem solchen Benutzer oder von der dritten Person nicht geändert werden. Aus dem gleichen Grund kann der Benutzer nicht die Rolle der Systemverwaltung durch unberechtigtes Auslesen oder Ändern der Systemverwaltungskennummer übernehmen, weil ein Benutzer nicht zum Speicherbereich 101 für die Systemverwaltungskennummer zum Zwecke des Auslesens oder Einschreibens von Daten zugreifen kann.

3736190

Nummer: 37 36 190
Int. Cl.⁴: G 06 F 12/14
Anmeldetag: 26. Oktober 1987
Offenlegungstag: 5. Mai 1988

FIG. 1a

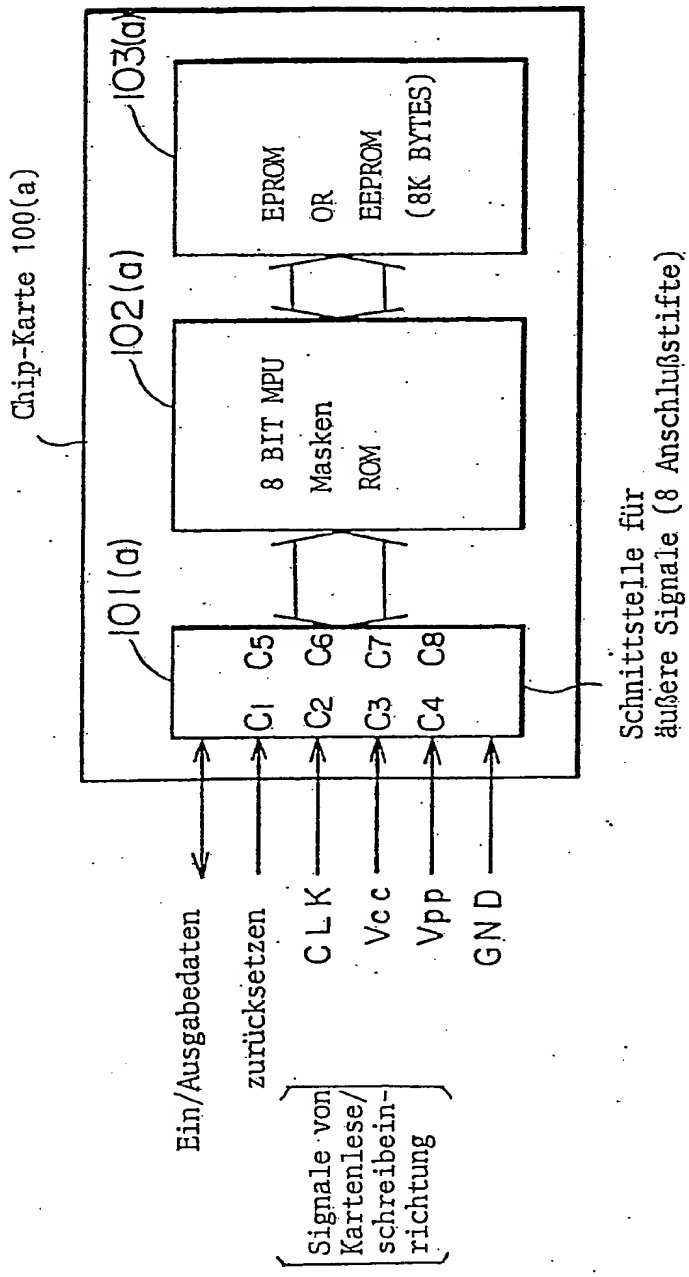


FIG. 1b

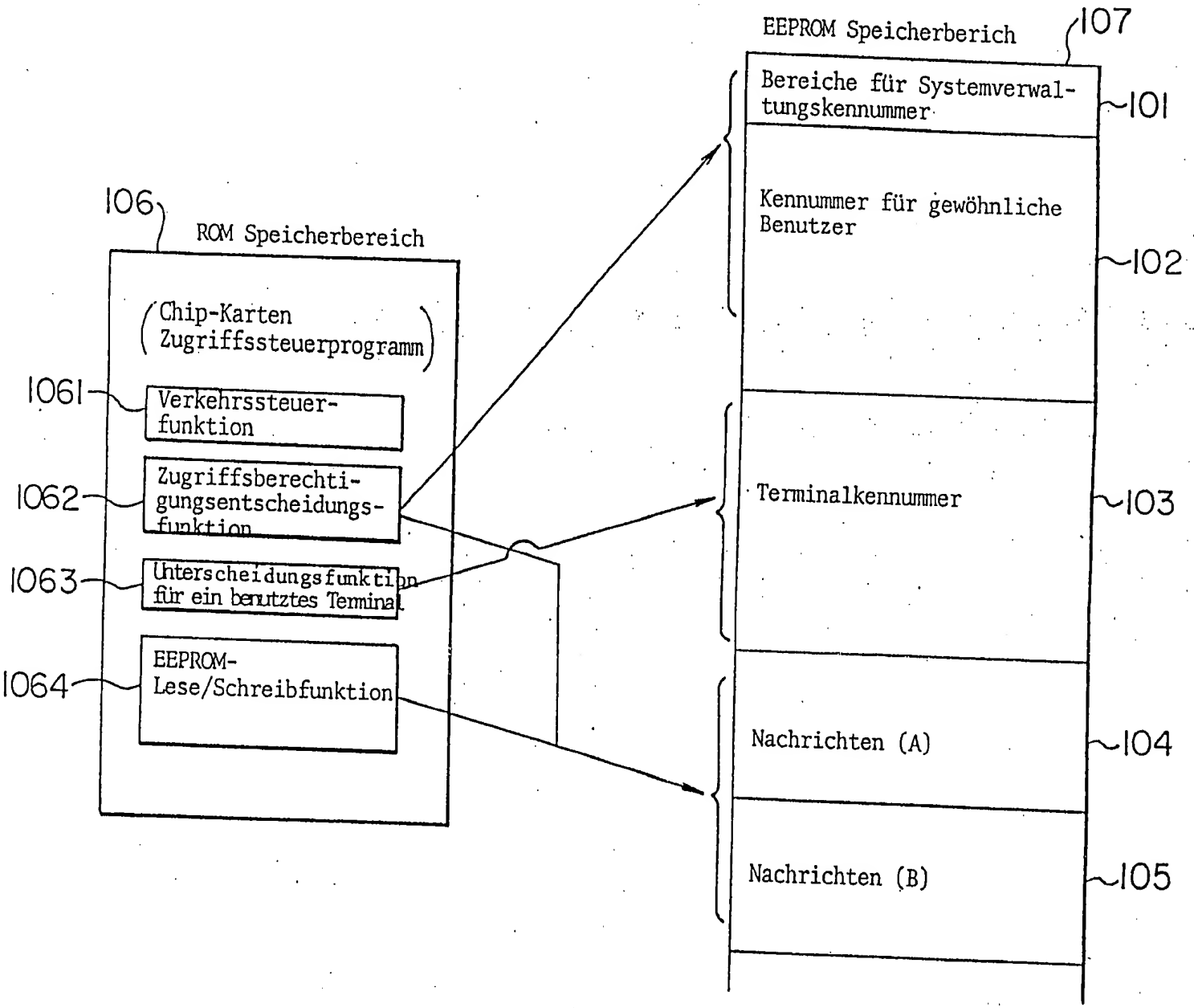


FIG. 2

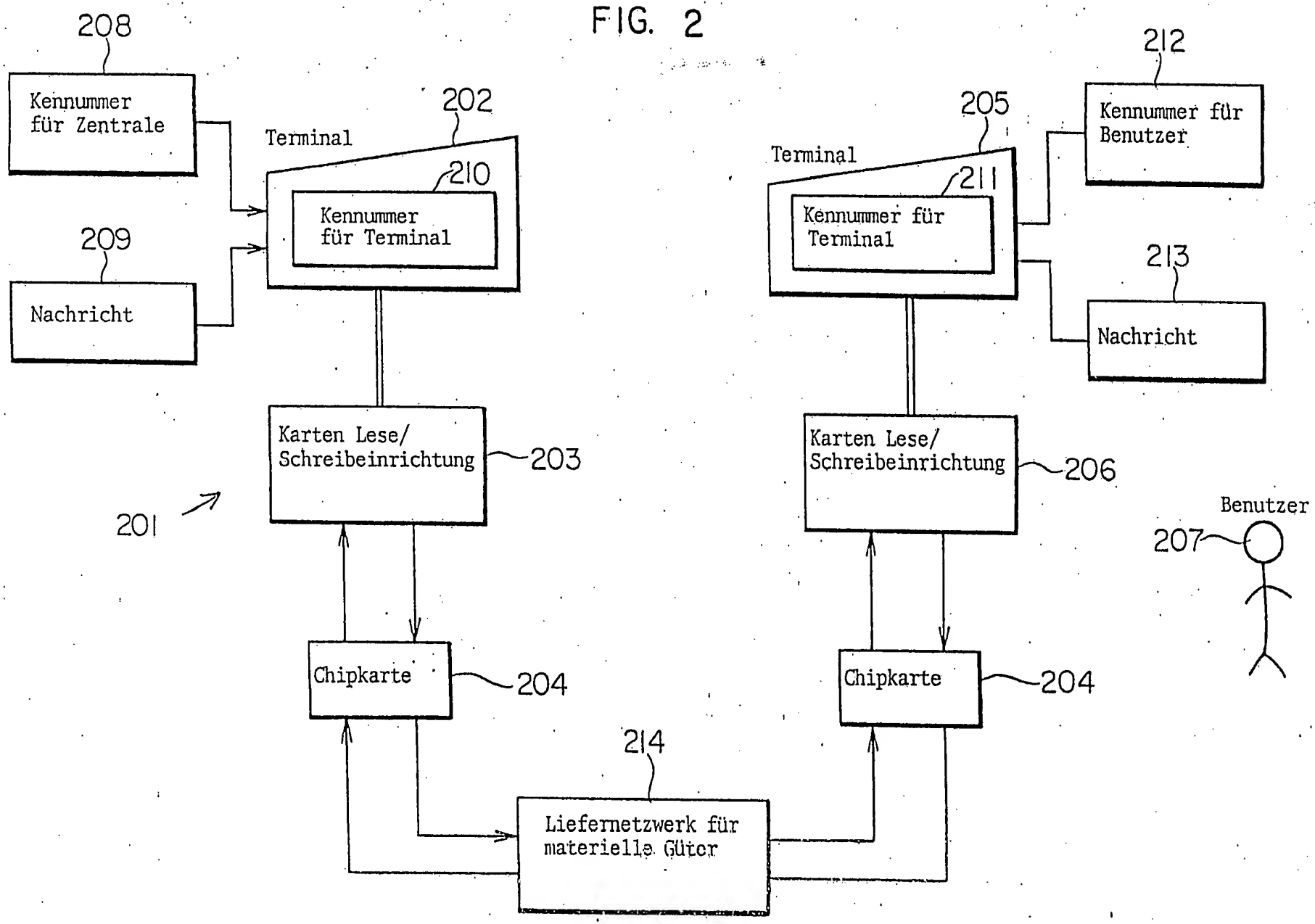
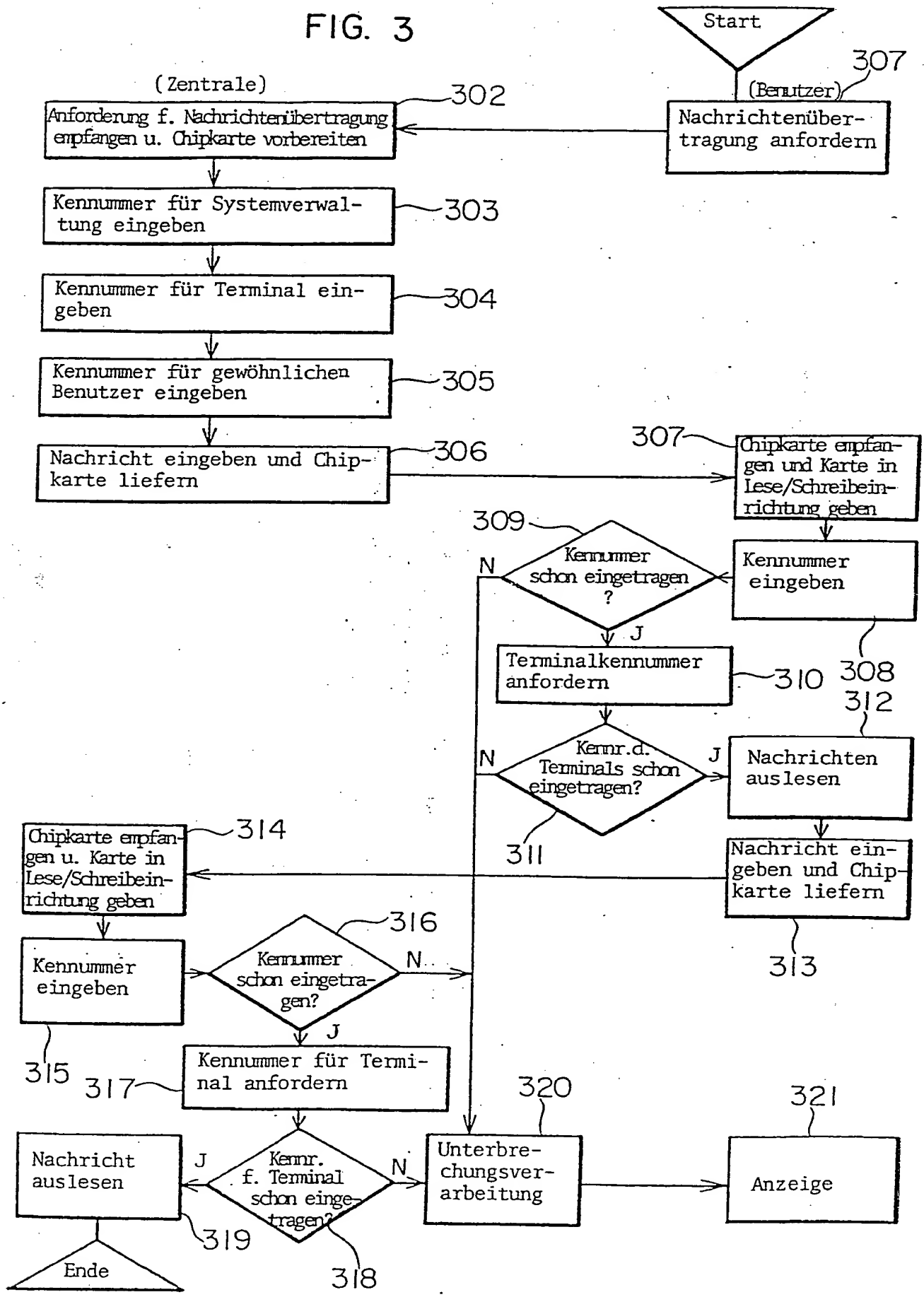


FIG. 3


Start
(Zentrale)
(Benutzer)
307
302
Anforderung f. Nachrichtenübertragung empfangen u. Chipkarte vorbereiten
Nachrichtenübertragung anfordern
Kennummer für Systemverwaltung eingeben
303
Kennummer für Terminal eingeben
304
Kennummer für gewöhnlichen Benutzer eingeben
305
Nachricht eingeben und Chipkarte liefern
306
307
Chipkarte empfangen und Karte in Lese/Schreibeinrichtung geben
309
Kennummer schon eingetragen ?
N
J
Kennummer eingeben
308
Terminalkennummer anfordern
310
312
Kennr.d. Terminals schon eingetragen?
N
J
311
Nachrichten auslesen
Chipkarte empfangen u. Karte in Lese/Schreibeinrichtung geben
314
Nachricht eingeben und Chipkarte liefern
313
316
Kennummer eingeben
Kennummer schon eingetragen?
N
J
315
317
Kennummer für Terminal anfordern
320
321
Nachricht auslesen
J
Kennr. f. Terminal schon eingetragen?
N
Unterbrechungsverarbeitung
Anzeige
319
318
Ende

B2438
13/5
米国

ACCESS CONTROL METHOD OF IC CARD

BACKGROUND OF THE INVENTION

The present invention relates to an access control method of information in a system in which a plurality of users utilize information stored in an IC card. An IC card comprises a plastic plate having a size identical to the size of a credit card in which one IC chip or plurality of IC chips is or are disposed.

In a method to use an IC card, the user possesses an IC card to be exclusively used by the user like a cash card and a credit card of the conventional system. Moreover, advantageously used the characteristic of the IC card, one IC card may be shared among a plurality of users like in a personal computer system.

In the usages of the IC card, when a plurality of users are assigned to an IC card, a memory of the IC card simultaneously includes information to be individually possessed by each user and information to be commonly used among the users. As a result, any user authourized to access the IC card has a chance to easily steal or alter the common information. Furthermore, even with a control of the access right by use of an identification number or the like, if some users do not appropriately observe the rule concerning the access right, the identification number may be known by

a third person, which possibly causes a damage or loss of information assigned to the users.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide an access control method of an IC card in a case where an IC card is utilized in a configuration in which a plurality of users exist, thereby improving the practicability in the usage of the IC card and solving the problems above.

According to the present invention, in order to guarantee the safety of the IC card utilization, there are introduced controls of the access right and the access range for the system manager and the ordinary user, respectively. The system manager here means a person who specifies the registration, deletion, access procedure, and access range for the ordinary user. The (ordinary) user is a person allowed to use an IC card according to the restriction imposed by the system manager. Moreover, the user also has own area and hence the right to access to the area by another user is also restricted.

According to the present invention, a virgin IC card delivered from a factory is subjected to an operation by the system manager for the registration of the system manager. This disables a person accessing thereafter to the IC card to be the system manager.

Next, the system manager effects registration

of users. In this operation, an area accessible by each user and procedures and restrictions for the users to access the IC card are also specified.

The specifications are implemented by an operation to write information such as identification numbers and the like of the users in an area which can be accessed only by the system manager. After these operation of initialization, the users are enabled to access the IC card.

When accessing the IC card, each user must follow the access procedures specified by the system manager, for example, to input an identification number unique to the user. Furthermore, even when the procedure is completed and the IC card is set to the accessible state, the user cannot access the areas other than those accessible areas specified by the system manager. That is, even when the user tries to rewrite data so as to remove the restrictions imposed on the user, this invalid operation is detected by the IC card, which accordingly takes a countermeasurement, for example, to lock the operation. Similarly, even when the user tries to steal information from the area accessible only by the system manager, the IC card can take an action, for example, to achieve processing to erase information.

With the control method above to prevent the steal and alteration of information, the message transmission as well as the secrecy and privacy control of information can be accomplished by means of the IC card.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram showing an example of the memory map of an IC card.

FIG. 2 is a block configuration diagram illustrating a configuration of a key delivery system.

FIG. 3 is a flowchart of a protocol of the key delivery.

DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 is a schematic diagram illustrating a configuration of an IC card according to the present invention. An IC card 100 (a) includes two LSI's. I/O data is communicated via an I/O section 101 (a) so as to be transferred to/from an EPROM (or EEPROM) section 103 (a) through a microprocessor 102 (a). The 8-bit MPU (microprocessor unit) 102 (a) includes therein a 4-kilobyte mask ROM for a program area. A program stored in the mask ROM is used to achieve a data communication with an external device and an access control on the data store memory (EPROM) 103 (a).

The EPROM 103 (a) is a nonvolatile memory storing the user data and has a capacity of eight kilobytes. This memory comprises an EPROM in which data is erased by an ultraviolet ray.

The EEPROM is an erasable, nonvolatile memory and has a capacity of eight kilobytes.

A description will be given of an embodiment of the present invention applied to a message exchange

operation.

FIG. 1 shows a memory map of an IC card in this embodiment. In this case, the area of the IC card is classified into an area accessible only by the system manager including a system manager identification number store area 101, an ordinary user identification number store area 102, and a terminal identification number store area 103 and an area accessible by both the system manager and the ordinary user including message store areas (A) 104 and (B) 105. The access right of the ordinary user can be arbitrarily determined by the system manager. The access right is limited to a message read operation for the message area (A) 104 and to message read and write operations for the message area (B) 105. Furthermore, the areas 101 - 105 are rewritable by use of an EEPROM or the like and the contents stored therein are controlled by an IC card access control program written in the ROM section 106. The control program is initiated by a command from a terminal and thereafter operations such as a retrieval and a judgment are accomplished by the control program, thereby controlling the contents stored in the EEPROM section 107.

That is, the command from the terminal is read by the I/O section 101 (a) of the smart card 100 (a) of FIG. 1 and is then decoded by the processor 102 (a), which causes the program to be executed beginning from the predetermined address of the ROM section 103 (a), namely, the first address thereof.

FIG. 2 shows an example of a configuration of a message exchange system implemented by use of the present invention.

FIG. 3 is a flowchart illustrating a processing procedure to effect a key delivery system in the configuration of FIG. 2 according to the present invention.

Next, referring to the flowchart of FIG. 3, a description will be given of the operations of the components of FIGS. 1 - 2.

Step 301

When requesting a message exchange, a user 207 supplies a center 201 with an identification number 212 of the user 207 and an identification number 211 of a terminal 205 to which a card reader/writer 206 is connected.

Step 302

The center 201 receives the message exchange request from the user 207 and then initiates preparing an IC card 204 for the message exchange.

Step 303

The center 201 writes an identification number 208 of the center 201 in a system manager identification number store area 101 of the IC card in the initial state. This causes the center 201 to be the system manager of the IC card.

Step 304

In order to restrict terminals accessible to the IC card 204, the center 201 writes an identification

number 210 of a terminal 202 in use and an identification number 211 of the terminal 205 operated by the user 207 in a terminal identification number store area 103 of the IC card 204.

Step 305

The center 201 writes the identification number 212 of the user in an ordinary user identification number store area 102 of the IC card.

Step 306

The center 201 writes a message in a message area (A) 104 of the IC card 204 and then delivers the IC card to the user 207 by use of a physical medium delivery network (for example, a registered mail).

Step 307

The user 207 receives the IC card 204 and thereafter installs the card 204 in the card R/W 206 connected to the terminal 205.

Step 308

The user 207 inputs the own identification number 212 to the IC card 204.

Step 309

An IC card access control program written in an ROM section 106 integrated in the IC card 204 searches the ordinary user identification number store area 102 for a check to determine whether or not the identification number 212 of the user 207 has already been registered thereto.

Step 310

If the identification number 212 has been registered, the control program requests the terminal 205 to send the terminal identification number 211.

Step 311

The control program searches the terminal identification number store area 103 for a check to determine whether or not the terminal identification number 211 of the terminal 205 operated by the user 207 has already been registered.

Step 312

If the identification number 211 has been registered, the user 207 reads the message 209 written in the message store area (A) 104 of the IC card 204.

Step 313

The user writes a message 213 of the user in a message area (B) 105 of the IC card 204 and then delivers the IC card 204 to the center 201 by use of the physical medium delivery network 214.

Step 314

The center 201 receives the IC card 204 and thereafter installs the card 204 in the card R/W 203 connected to the terminal 202.

Step 315

The center 201 inputs the own identification number 208 to the IC card 204.

Step 316

The control program effects a check to determine

whether or not the identification number 201 of the center has already been registered to the system manager identification number store area 101.

Step 317

If the identification number 208 has been registered, the control program requests the terminal 202 to transmit the terminal identification number 210.

Step 318

The control program searches the terminal identification number store area 103 for a check to determine whether or not the terminal identification number 210 of the center 201 has already been registered.

Step 319

If the terminal identification number 210 has been registered, the center 201 reads the message 213 from the message store area (B) 105 of the IC card 204.

Incidentally, if the check results in a non-registered state in the steps 309, 311, 316, and 319, control jumps to step 320 to interrupt the processing and then step 321 is executed to notify the condition to the user 207.

According to the present invention, there will be attained the following effects.

(1) Prevention of the steal and alteration of data in a course of the card delivery

When the IC card is delivered by use of a physical medium delivery network such as the mail, the IC card may possibly be passed to a third person

having a malicious intent in a route of the delivery. In such a case, since the IC card checks by itself the identification number, the terminal identification number, and the like as described in conjunction with the steps 309, 311, 316, and 318, the third person not knowing the check cannot access the IC card. Consequently, the steal and alteration of the data in the delivery route can be prevented.

(2) Prevention of alteration of a center message by the user

The (ordinary) user or a third person knowing the ordinary user identification number, the terminal identification number, and the like registered to the IC card can access the IC card accordingly. However, since the center message is written in an area accessible only by the system manager, the message cannot be altered by such a user nor by the third person. For the similar reason, since the system manager identification number store area 101 is prevented from being accessed (for a data read write operations) by the user; consequently, the user cannot become a system manager by stealing or altering the system manager identification number.

CLAIMS:

1. A control method of an IC card having a data input/output section, a data processing section, and a data store section to be accessed by a plurality of users wherein

a first user sets for another user an access procedure and an accessible range of the IC card.

2. A control method according to Claim 1 wherein

said first user is a user first accessing the IC card and

another user subsequently attempting to access the IC card is enabled to access the IC card when said another user executes the access procedure or within the accessible range specified by said first user.

3. A control method according to Claim 1 wherein said access procedure and said accessible range can be set only by said first user.

4. A control method according to Claim 1 wherein when said another user tries to alter the access procedure or the accessible range beforehand set, a lock of the operation, an erasure of data, or an inversion of an invalidity detection bit is effected as a counter-measurement.

5. A control method according to Claim 1 wherein said first user is a manager of a system using said IC card.

ABSTRACT OF THE DISCLOSURE

In order to improve the reliability of a system in which an IC card is used by a plurality of users, only the user first accessing the virgin IC card delivered from a firm can set an access procedure and an accessible range of the IC card. The second and subsequent users use the IC card according to the access procedure and the accessible range thus established.

FIG. 1

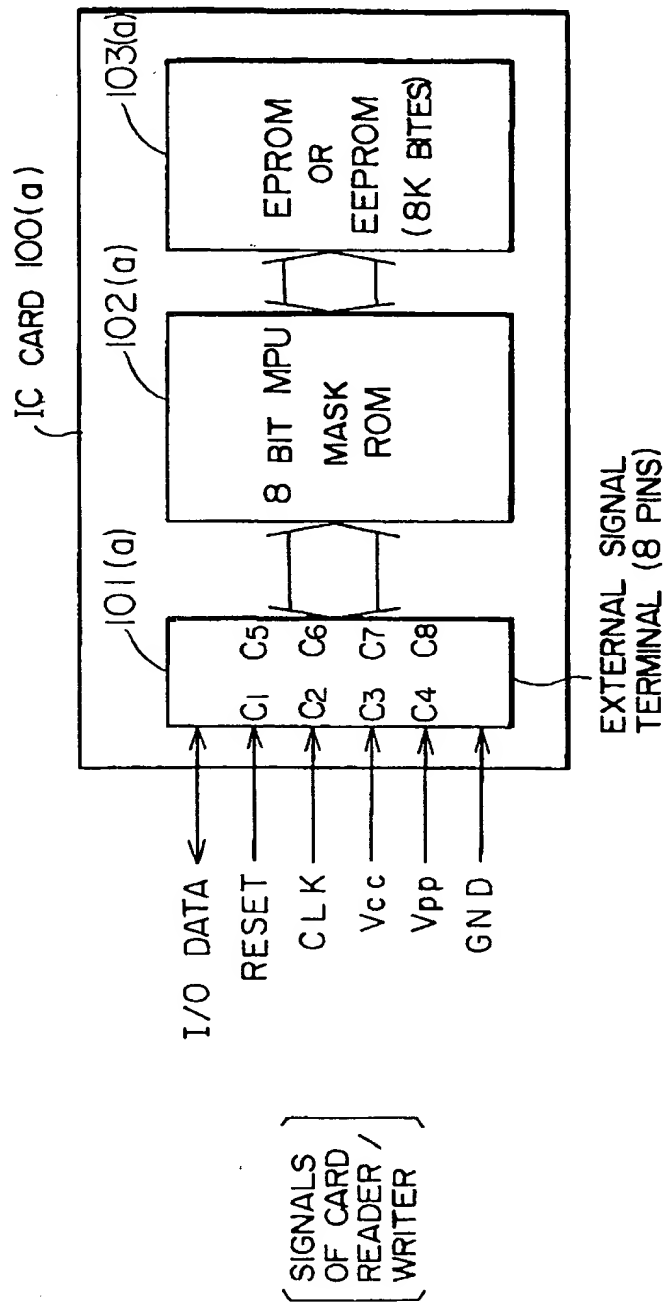

IC CARD 100(a)
101(a)
102(a)
103(a)
8 BIT MPU
MASK
ROM
EPROM
OR
EEPROM
(8K BITES)
C1
C2
C3
C4
C5
C6
C7
C8
EXTERNAL SIGNAL
TERMINAL (8 PINS)
I/O DATA
RESET
CLK
Vcc
Vpp
GND
SIGNALS
OF CARD
READER /
WRITER

FIG. 2

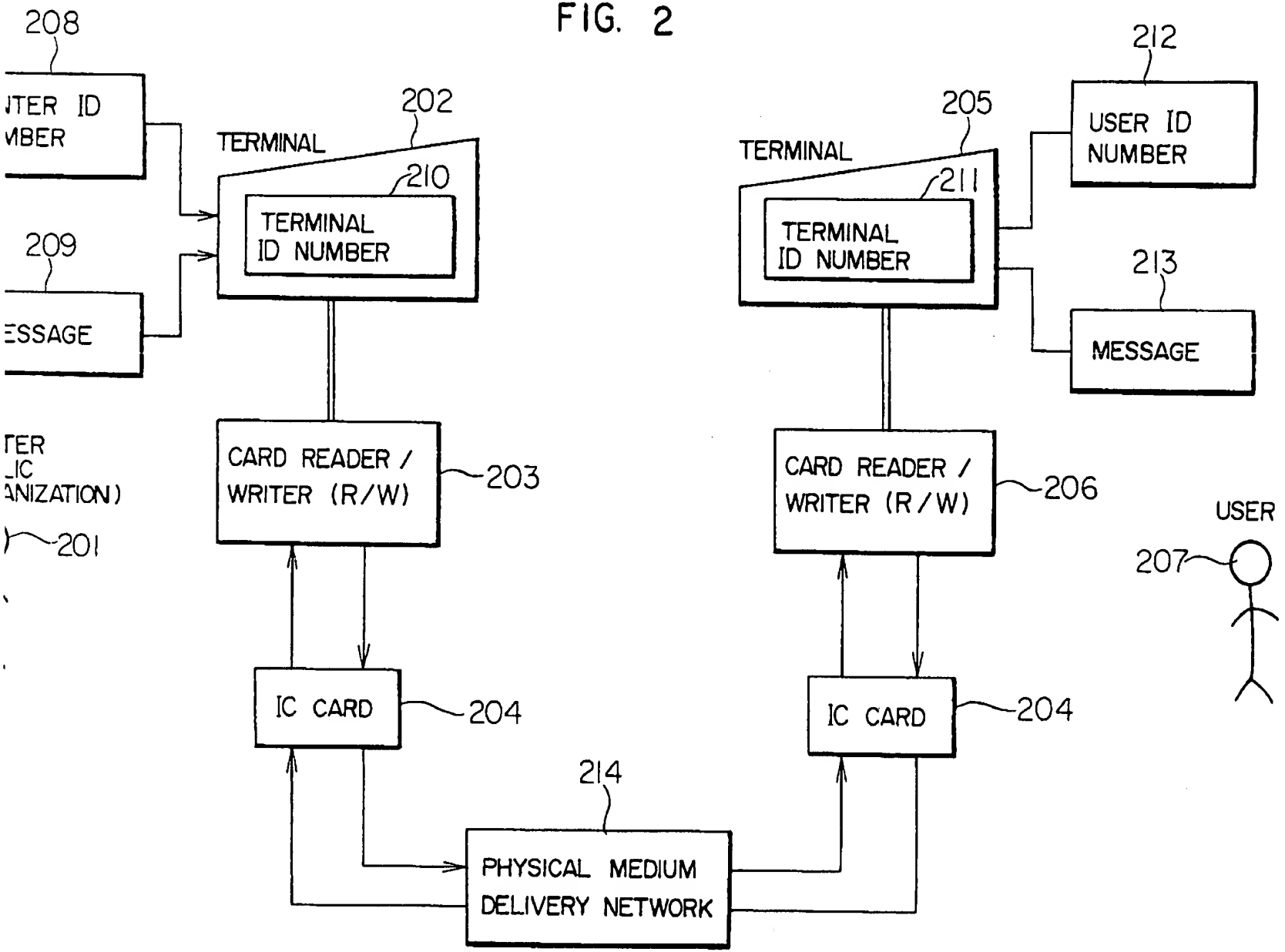
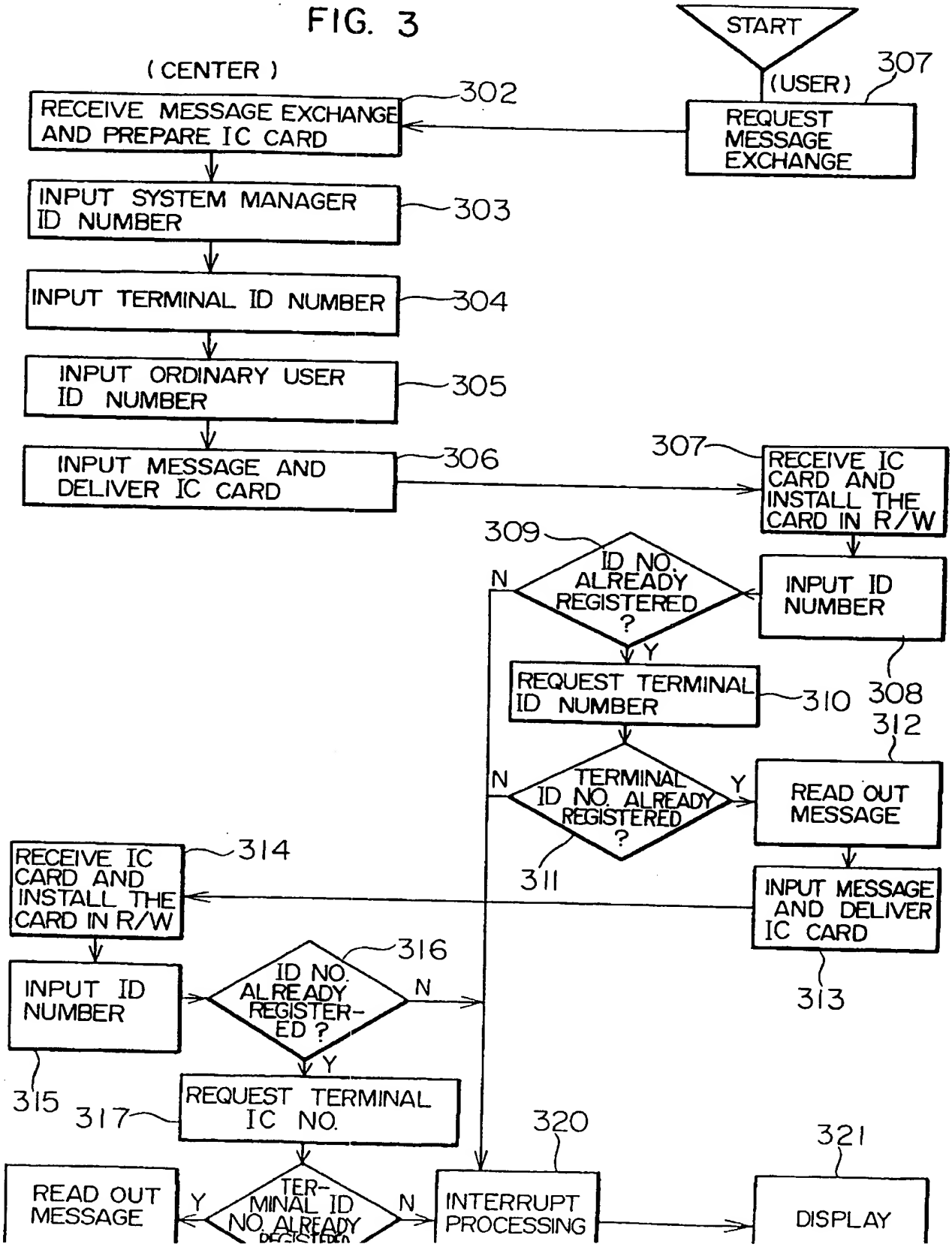

208
JTER ID
MBER
209
ESSAGE
TER
IC
ANIZATION)
201
TERMINAL
202
210
TERMINAL
ID NUMBER
CARD READER /
WRITER (R/W)
203
IC CARD
204
214
PHYSICAL MEDIUM
DELIVERY NETWORK
TERMINAL
205
211
TERMINAL
ID NUMBER
212
USER ID
NUMBER
213
MESSAGE
CARD READER /
WRITER (R/W)
206
USER
207
IC CARD
204

FIG. 3


START
(CENTER)
(USER)
307
302
RECEIVE MESSAGE EXCHANGE AND PREPARE IC CARD
REQUEST MESSAGE EXCHANGE
INPUT SYSTEM MANAGER ID NUMBER
303
INPUT TERMINAL ID NUMBER
304
INPUT ORDINARY USER ID NUMBER
305
INPUT MESSAGE AND DELIVER IC CARD
306
307
RECEIVE IC CARD AND INSTALL THE CARD IN R/W
309
ID NO. ALREADY REGISTERED ?
N
Y
INPUT ID NUMBER
308
REQUEST TERMINAL ID NUMBER
310
312
TERMINAL ID NO. ALREADY REGISTERED ?
N
Y
READ OUT MESSAGE
311
INPUT MESSAGE AND DELIVER IC CARD
313
314
RECEIVE IC CARD AND INSTALL THE CARD IN R/W
INPUT ID NUMBER
316
ID NO. ALREADY REGISTER-ED ?
N
Y
315
317
REQUEST TERMINAL IC NO.
320
321
READ OUT MESSAGE
Y
TER-MINAL ID NO. ALREADY
N
INTERRUPT PROCESSING
DISPLAY